NANYANG TECHNOLOGICAL UNIVERSITY

Inaugural Youth Olympic Village

256 Bit Standardized Crypto for 650 GE - GOST Revisited

A. Poschmann, S. Ling, and H. Wang

Axel Poschmann
Division of Mathematical Sciences,
School of Physical and Mathematical Sciences

18 August 2010

Outline

- **Introduction**
- GOST
- How to choose a set of S-boxes?
- Implementation Results
- Conclusions

Introduction

GOST = **GO**vernment **ST**andard
государственный **ст**андарт

In this talk we focus on GOST 28147-89

- **GOST 28147-89:**
  - Block cipher standardized in 1989
  - „Soviet cousin“ of DES
  - IETF draft
  - Discussed for inclusion in ISO 18033-3

Introduction

GOST = **GO**vernment **ST**andard
государственный **ст**андарт

In this talk we focus on GOST 28147-89

- **GOST 28147-89:**
  - Block cipher standardized in 1989
  - „Soviet cousin“ of DES
  - IETF draft
  - Discussed for inclusion in ISO 18033-3

- **21 years of cryptanalysis:**
  - Related-key DC breaks 21 rounds /w 2^{56} CP
  - Slide attack breaks 24 rounds /w 2^{63} CP (30 when S-boxes are known)
  - Reflection attack on full-round GOST /w 2^{32} CP and time 2^{192}
  (assumes bijective S-boxes, works only on 2^{224} keys)

Introduction

GOST = **GO**vernment **ST**andard
государственный **ст**андарт

In this talk we focus on GOST 28147-89

- **GOST 28147-89:**
  - Block cipher standardized in 1989
  - „Soviet cousin“ of DES
  - IETF draft
  - Discussed for inclusion in ISO 18033-3

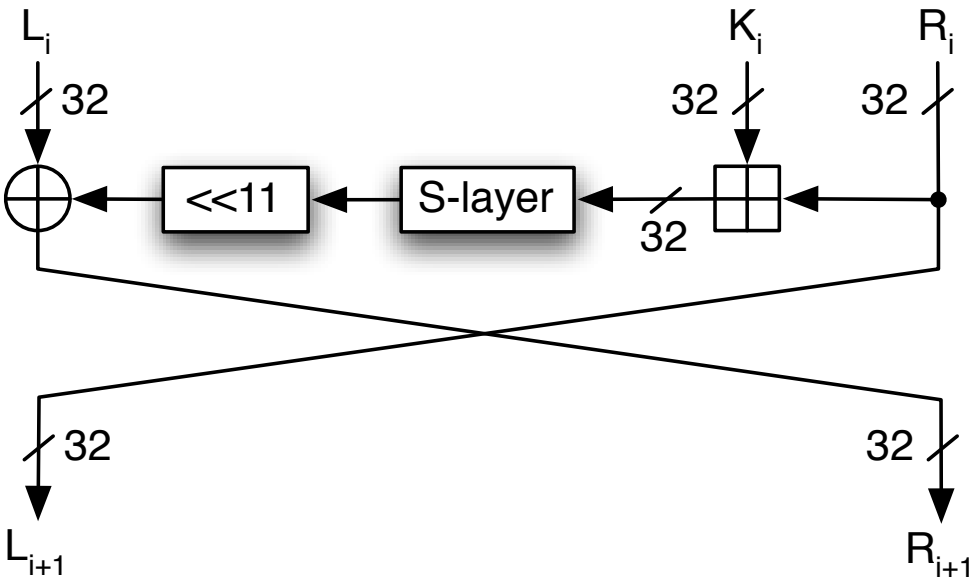
- **21 years of cryptanalysis:**
  - Related-key DC breaks 21 rounds /w 2^{56} CP
  - Slide attack breaks 24 rounds /w 2^{63} CP (30 when S-boxes are known)
  - Reflection attack on full-round GOST /w 2^{32} CP and time 2^{192}
  (assumes bijective S-boxes, works only on 2^{224} keys)

2010 GOST is still secure!

Outline

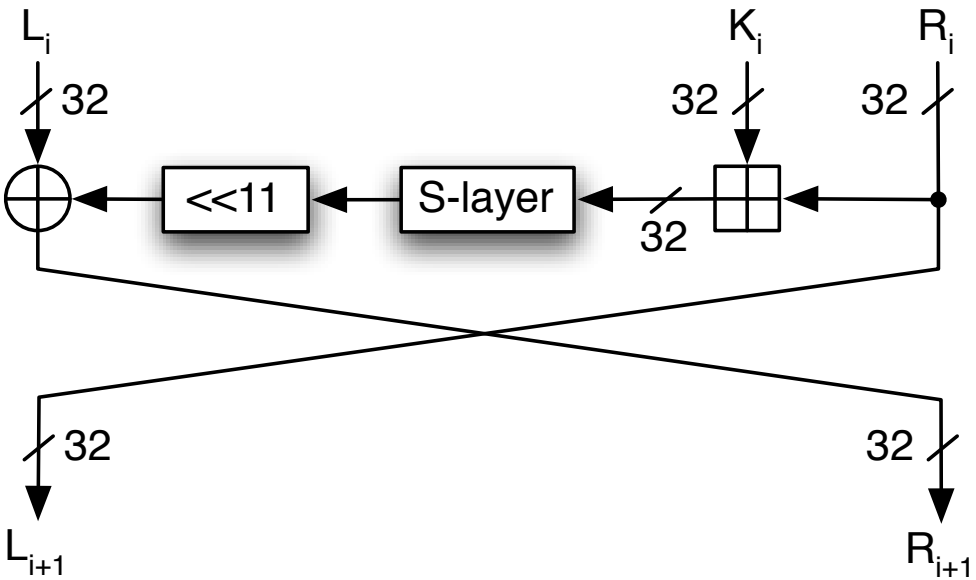
- Introduction
- **GOST**
- How to choose a set of S-boxes?
- Implementation Results
- Conclusions

GOST I



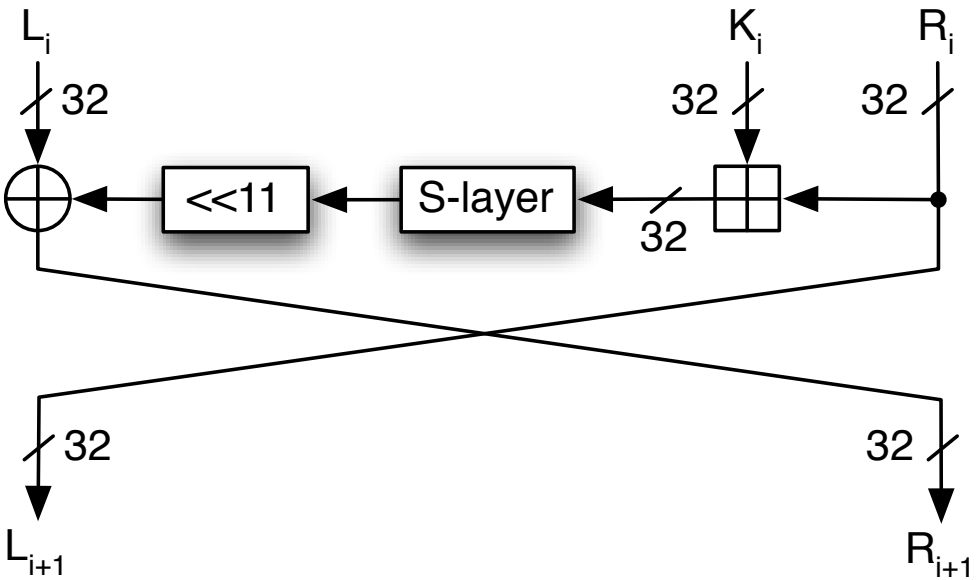
- 2 branch Feistel Network
- 32 rounds
- 64-bit block size
- 256-bit key length
- $K=K_0||K_1||K_2||K_3||K_4||K_5||K_6||K_7$
- No key schedule

GOST I



- 2 branch Feistel Network
- 32 rounds
- 64-bit block size
- 256-bit key length
- $K = K_0 || K_1 || K_2 || K_3 || K_4 || K_5 || K_6 || K_7$
- No key schedule

GOST I

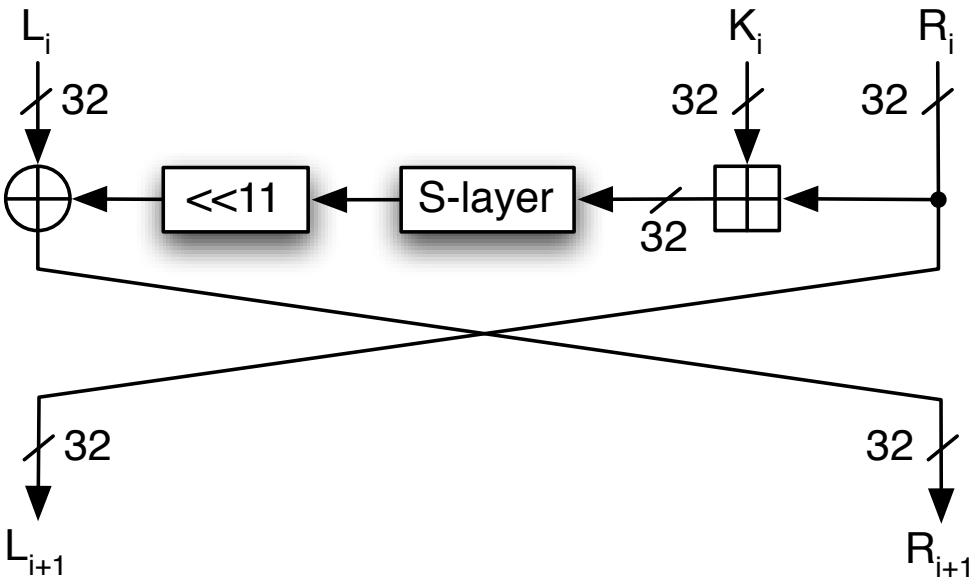


- 2 branch Feistel Network
- 32 rounds
- 64-bit block size
- 256-bit key length
- $K = K_0 || K_1 || K_2 || K_3 || K_4 || K_5 || K_6 || K_7$
- No key schedule

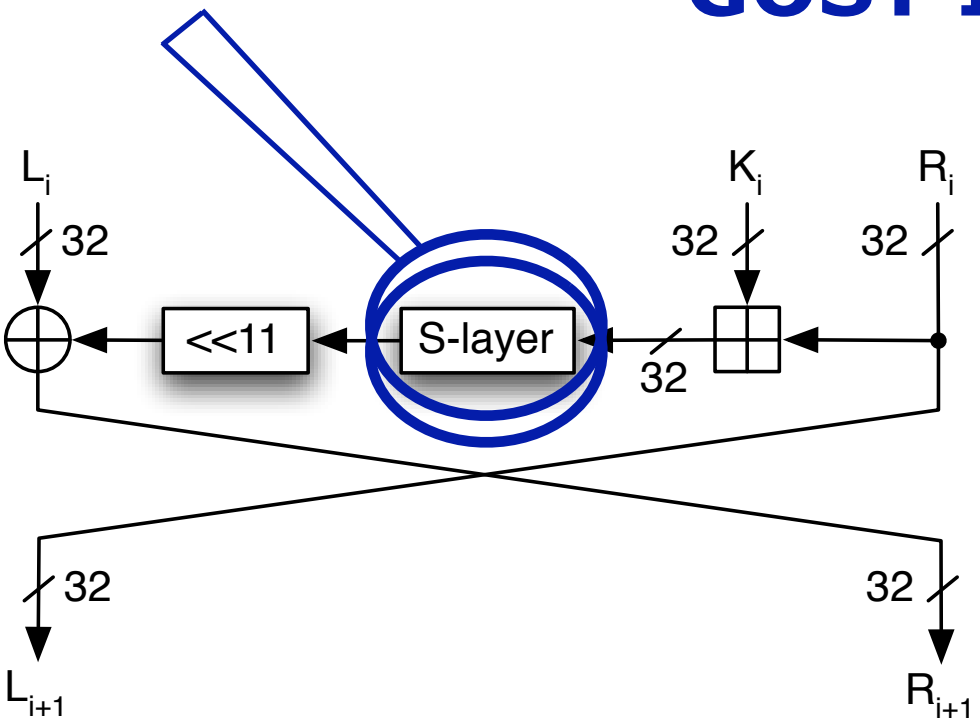
Round	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Key	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
Round	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Key	K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_7	K_6	K_5	K_4	K_3	K_2	K_1	K_0

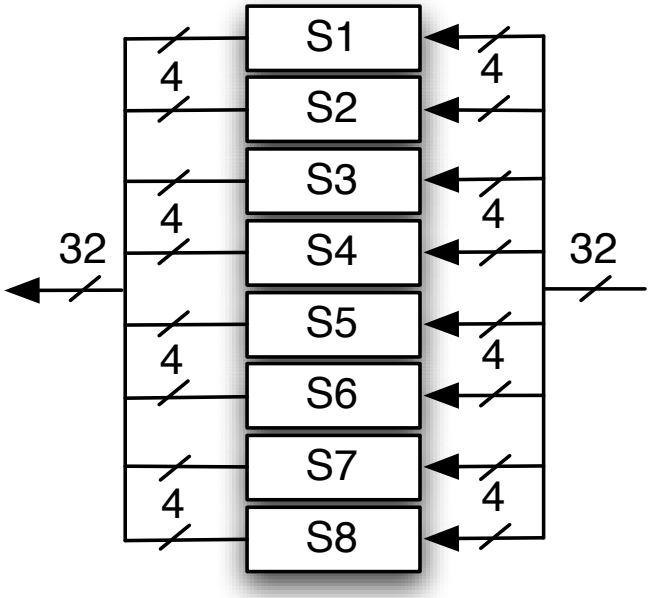
Reverse Order!

GOST II

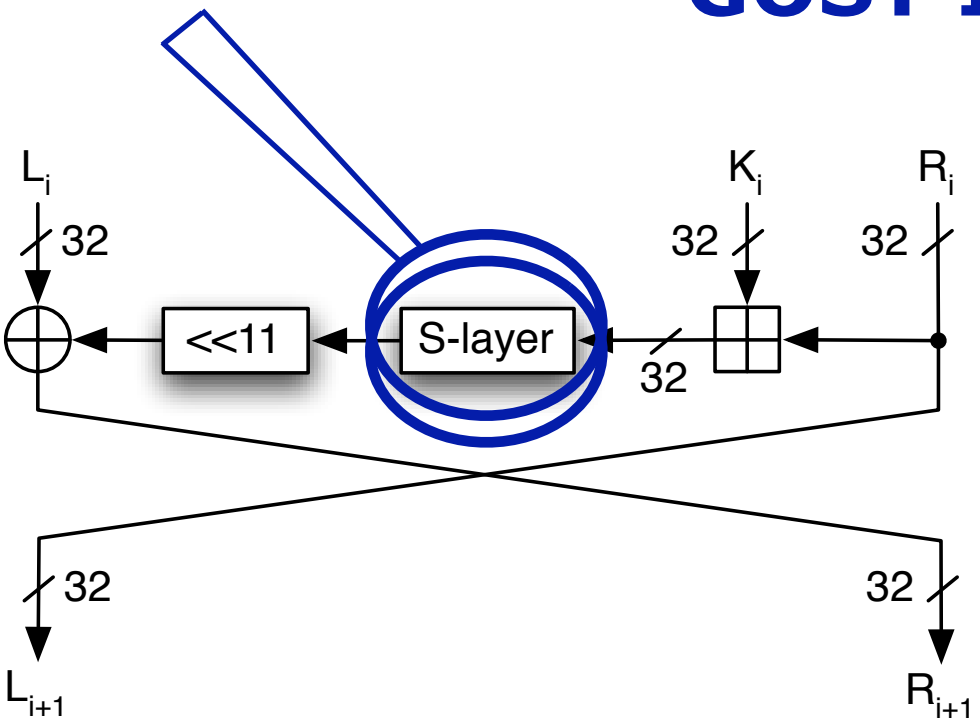


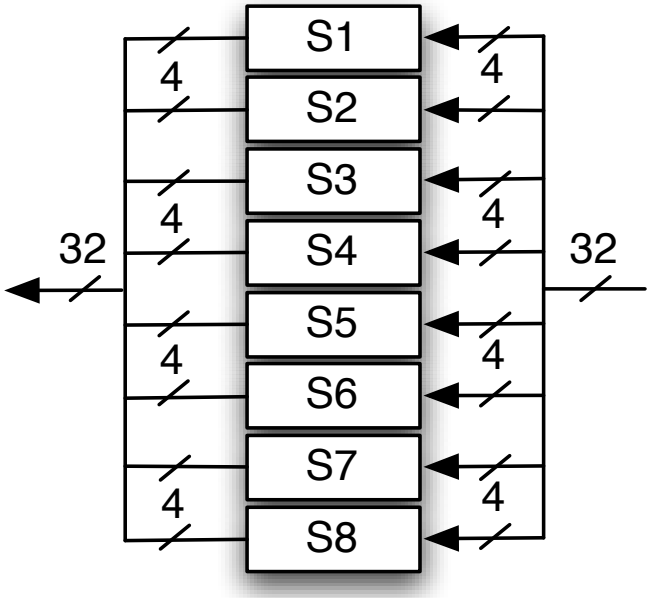
GOST II


L_i
32
K_i
32
R_i
32
<<11
S-layer
32
32
32
L_{i+1}
R_{i+1}


S1
S2
S3
S4
S5
S6
S7
S8
4
32
32

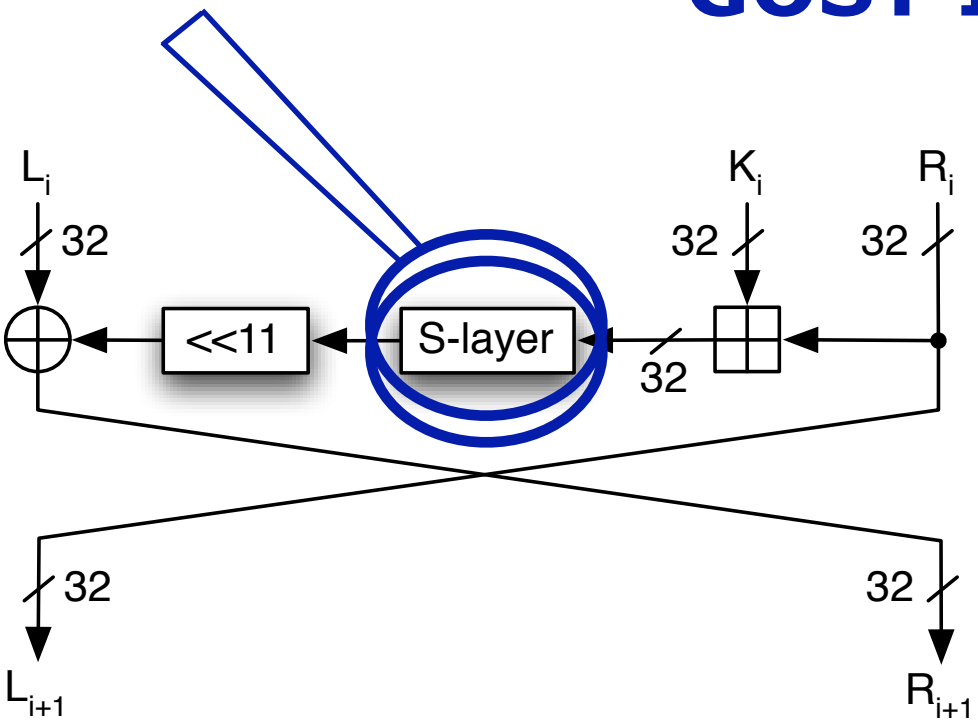
GOST II

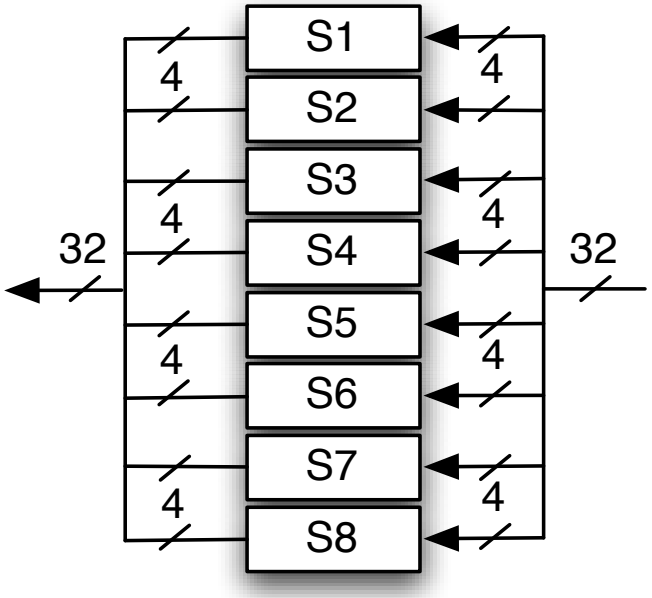




S-boxes not specified!

GOST II

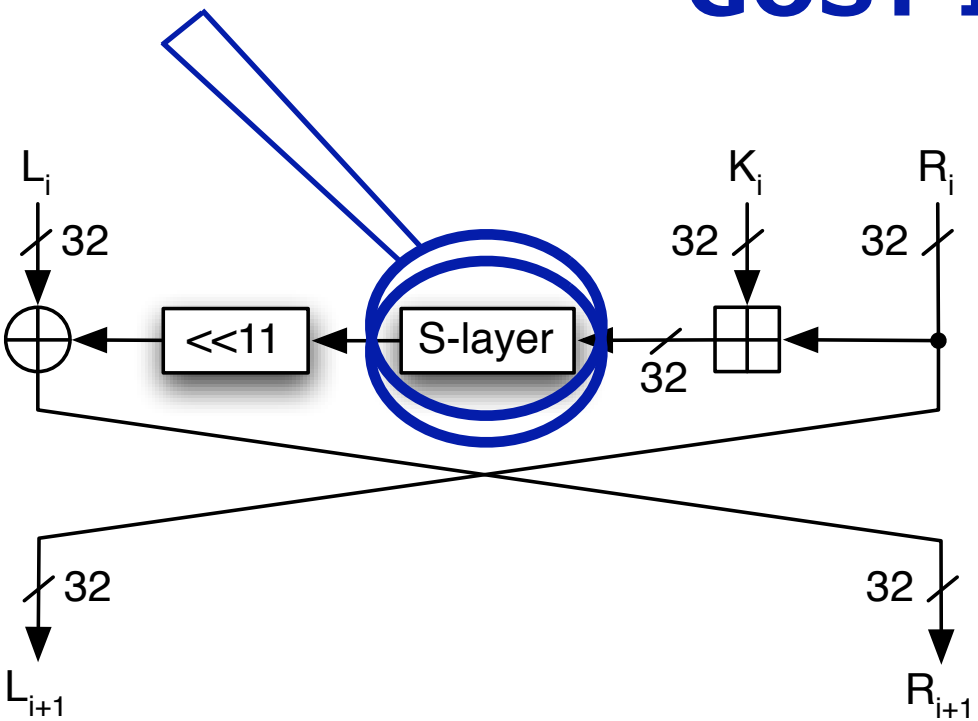


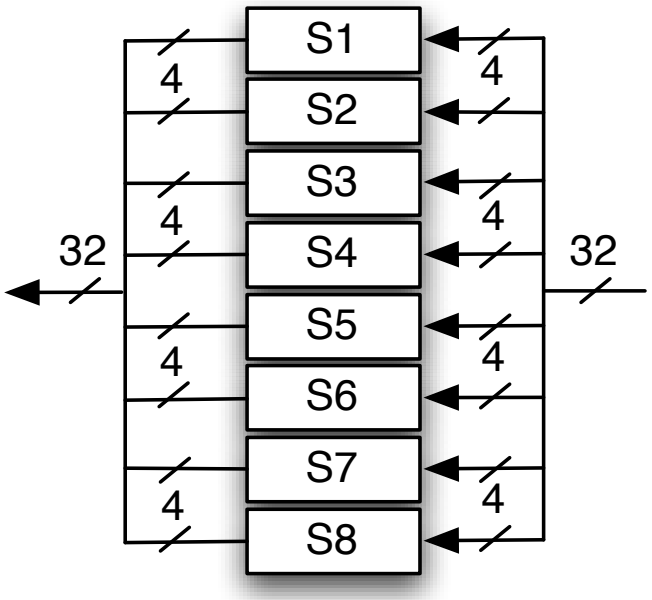


- Design goal: flexible security level (possibly security concerns)
- Selection of S-boxes is part of key
- $2^8 \cdot 16!$ possible sets
- => 354 additional key bits
- But! set revealed by 2^{32} chosen keys
- No restrictions for S-boxes

S-boxes not specified!

GOST II





- Design goal: flexible security level (possibly security concerns)
- Selection of S-boxes is part of key
- $2^8 \cdot 16!$ possible sets
- => 354 additional key bits
- But! set revealed by 2^{32} chosen keys
- No restrictions for S-boxes

S-boxes not specified!

Proper choice of S-boxes is crucial!

Outline

- Introduction
- GOST
- **How to choose a set of S-boxes?**
- Implementation Results
- Conclusions

A Proper Choice

One example are the S-boxes used by the Central Bank of Russian Federation

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S_1(x)$	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5	3
$S_2(x)$	E	B	4	C	6	D	F	A	2	3	8	1	0	7	5	9
$S_3(x)$	5	8	1	D	A	3	4	2	E	F	C	7	6	0	9	B
$S_4(x)$	7	D	A	1	0	8	9	F	E	4	6	C	B	2	5	3
$S_5(x)$	6	C	7	1	5	F	D	8	4	A	9	E	0	3	B	2
$S_6(x)$	4	B	A	0	7	2	1	D	3	6	8	5	9	C	F	E
$S_7(x)$	D	B	4	1	3	F	5	9	0	A	E	7	6	8	2	C
$S_8(x)$	1	F	D	0	5	7	A	4	9	2	3	E	6	B	8	C

A Proper Choice

One example are the S-boxes used by the Central Bank of Russian Federation

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S_1(x)$	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5	3
$S_2(x)$	E	B	4	C	6	D	F	A	2	3	8	1	0	7	5	9
$S_3(x)$	5	8	1	D	A	3	4	2	E	F	C	7	6	0	9	B
$S_4(x)$	7	D	A	1	0	8	9	F	E	4	6	C	B	2	5	3
$S_5(x)$	6	C	7	1	5	F	D	8	4	A	9	E	0	3	B	2
$S_6(x)$	4	B	A	0	7	2	1	D	3	6	8	5	9	C	F	E
$S_7(x)$	D	B	4	1	3	F	5	9	0	A	E	7	6	8	2	C
$S_8(x)$	1	F	D	0	5	7	A	4	9	2	3	E	6	B	8	C

Another **standard conform** example is to use 8 times the PRESENT S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

A Proper Choice

One example are the S-boxes used by the Central Bank of Russian Federation

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	max S_b^W	max DC
$S_1(x)$	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5	3	8	6
$S_2(x)$	E	B	4	C	6	D	F	A	2	3	8	1	0	7	5	9	12	6
$S_3(x)$	5	8	1	D	A	3	4	2	E	F	C	7	6	0	9	B	12	6
$S_4(x)$	7	D	A	1	0	8	9	F	E	4	6	C	B	2	5	3	12	6
$S_5(x)$	6	C	7	1	5	F	D	8	4	A	9	E	0	3	B	2	12	4
$S_6(x)$	4	B	A	0	7	2	1	D	3	6	8	5	9	C	F	E	12	6
$S_7(x)$	D	B	4	1	3	F	5	9	0	A	E	7	6	8	2	C	12	8
$S_8(x)$	1	F	D	0	5	7	A	4	9	2	3	E	6	B	8	C	12	8

Another **standard conform** example is to use 8 times the PRESENT S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2	**8**	**4**

A Proper Choice

One example are the S-boxes used by the Central Bank of Russian Federation

GOST-FB

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	max S_b^W	max DC
$S_1(x)$	4	A	9	2	D	8	0	E	6	B	1	C	7	F	5	3	8	6
$S_2(x)$	E	B	4	C	6	D	F	A	2	3	8	1	0	7	5	9	12	6
$S_3(x)$	5	8	1	D	A	3	4	2	E	F	C	7	6	0	9	B	12	6
$S_4(x)$	7	D	A	1	0	8	9	F	E	4	6	C	B	2	5	3	12	6
$S_5(x)$	6	C	7	1	5	F	D	8	4	A	9	E	0	3	B	2	12	4
$S_6(x)$	4	B	A	0	7	2	1	D	3	6	8	5	9	C	F	E	12	6
$S_7(x)$	D	B	4	1	3	F	5	9	0	A	E	7	6	8	2	C	12	8
$S_8(x)$	1	F	D	0	5	7	A	4	9	2	3	E	6	B	8	C	12	8

Another **standard conform** example is to use 8 times the PRESENT S-box

GOST-PS

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2	**8**	**4**

Outline

- Introduction
- GOST
- How to choose a set of S-boxes?
- **Implementation Results**
- Conclusions

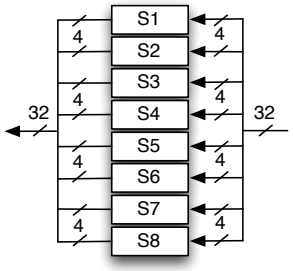
Implementation Comments

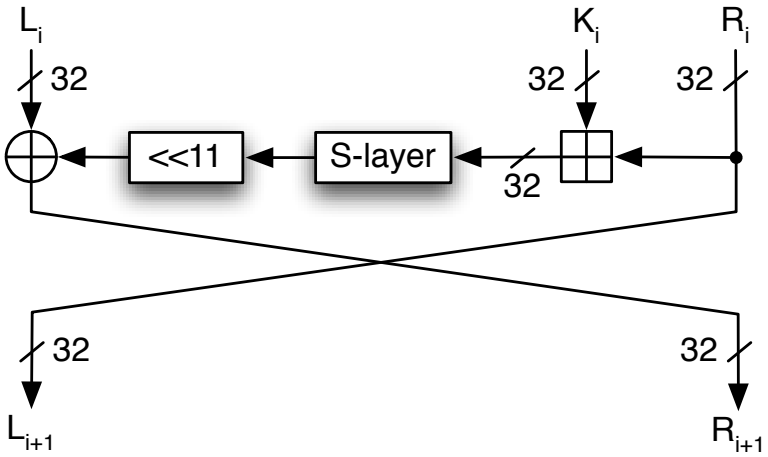
- In RFID scenarios key is most likely fixed
  - store key in EEPROM etc
  - hardwire key
- if key update needed
  - additional 256 FF required

Implementation Results I

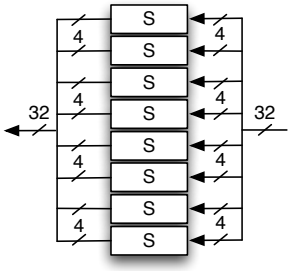
UMCL18G212T3 library

GOST-FB





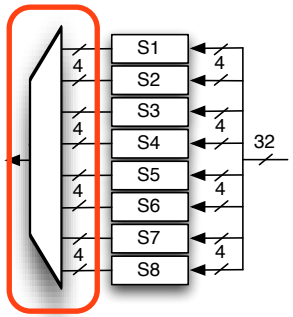
GOST-PS

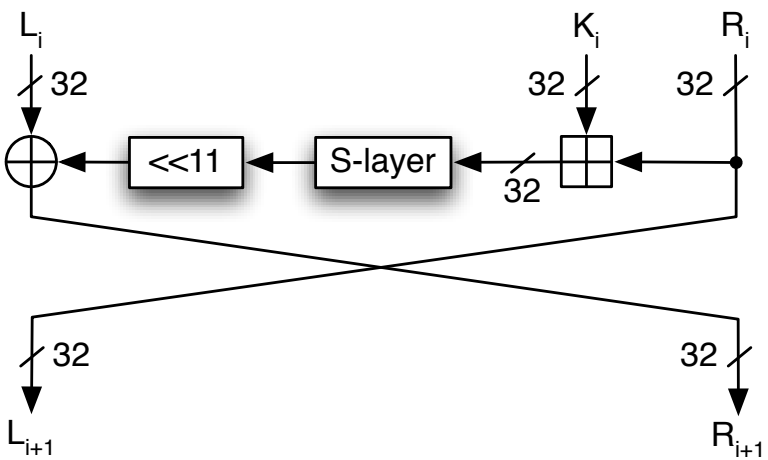


Implementation Results I

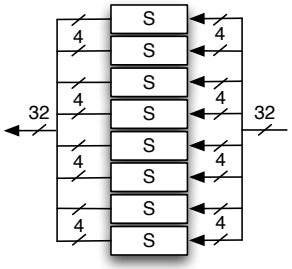
UMCL18G212T3 library

GOST-FB





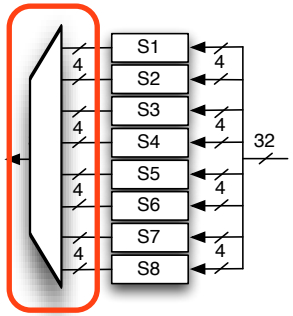
GOST-PS

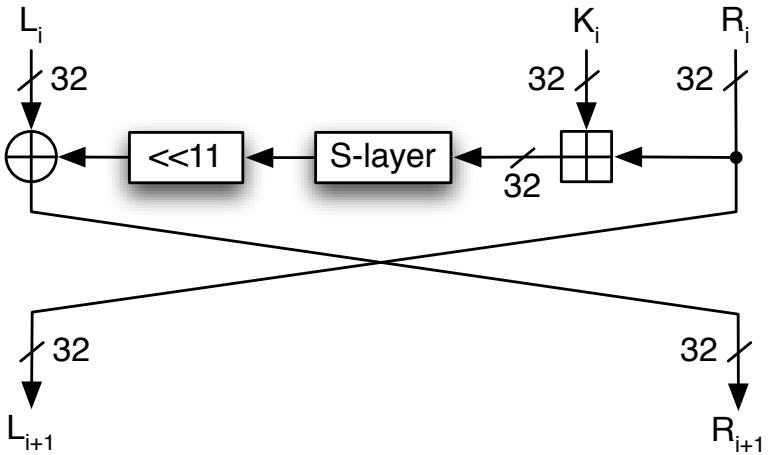


Implementation Results I

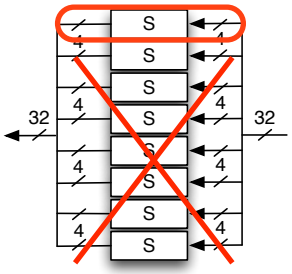
UMCL18G212T3 library

GOST-FB





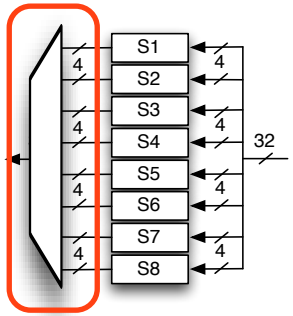
GOST-PS

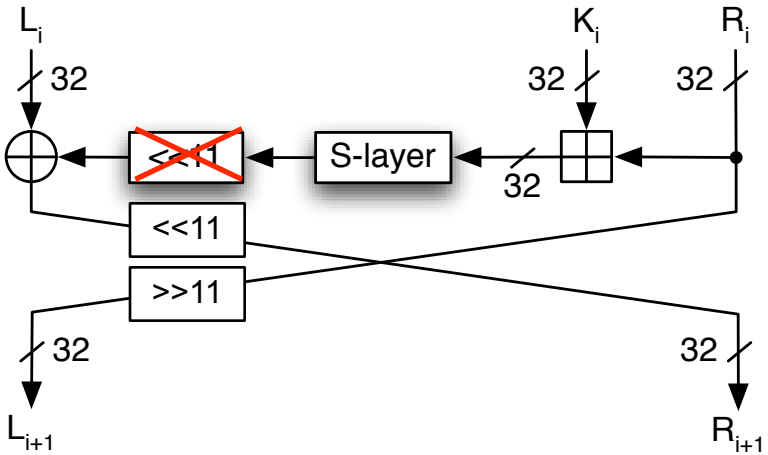


Implementation Results I

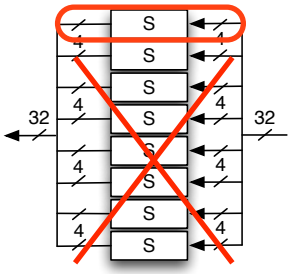
UMCL18G212T3 library

GOST-FB





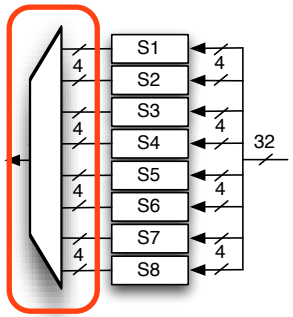
GOST-PS

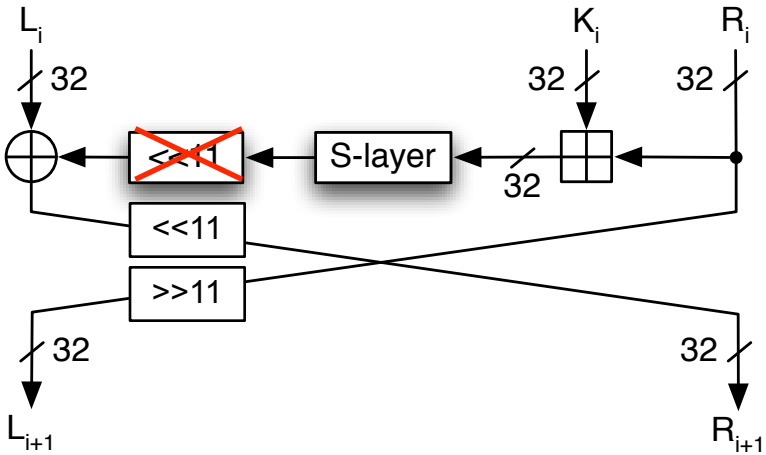


Implementation Results I

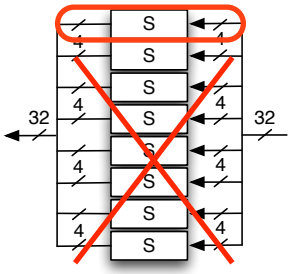
UMCL18G212T3 library

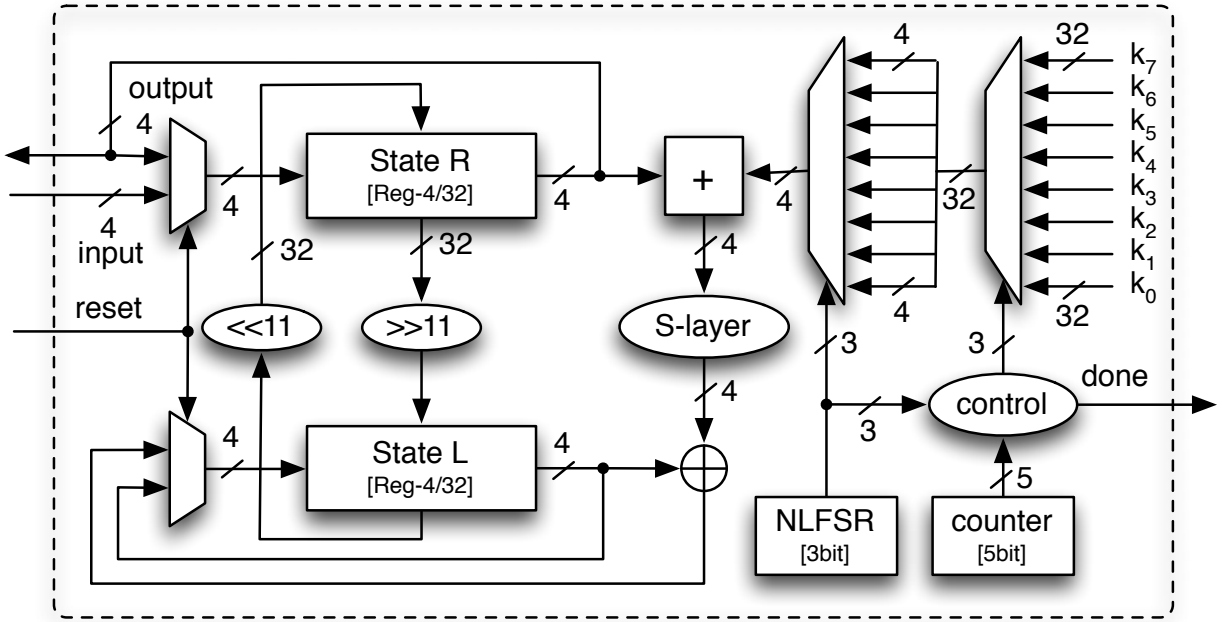
GOST-FB





GOST-PS

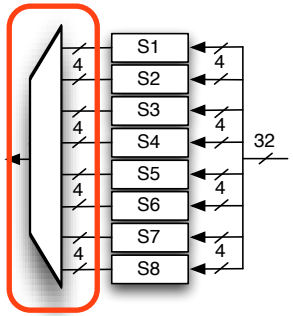


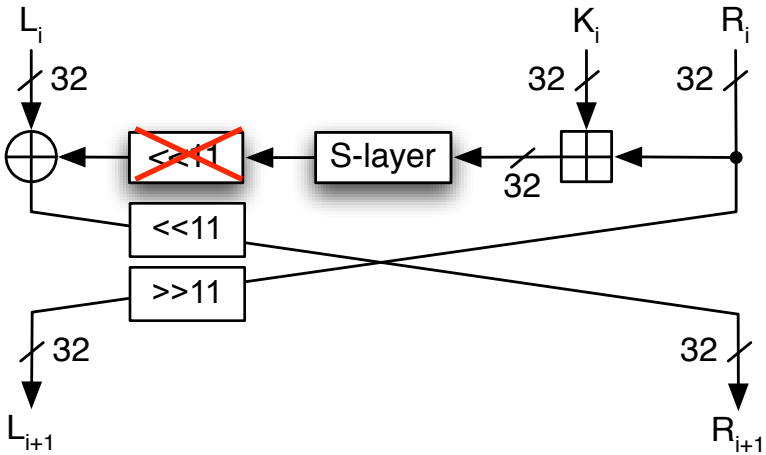


Implementation Results I

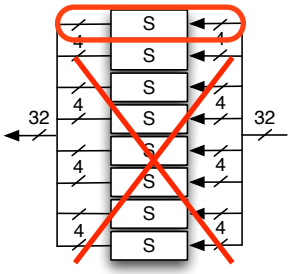
UMCL18G212T3 library

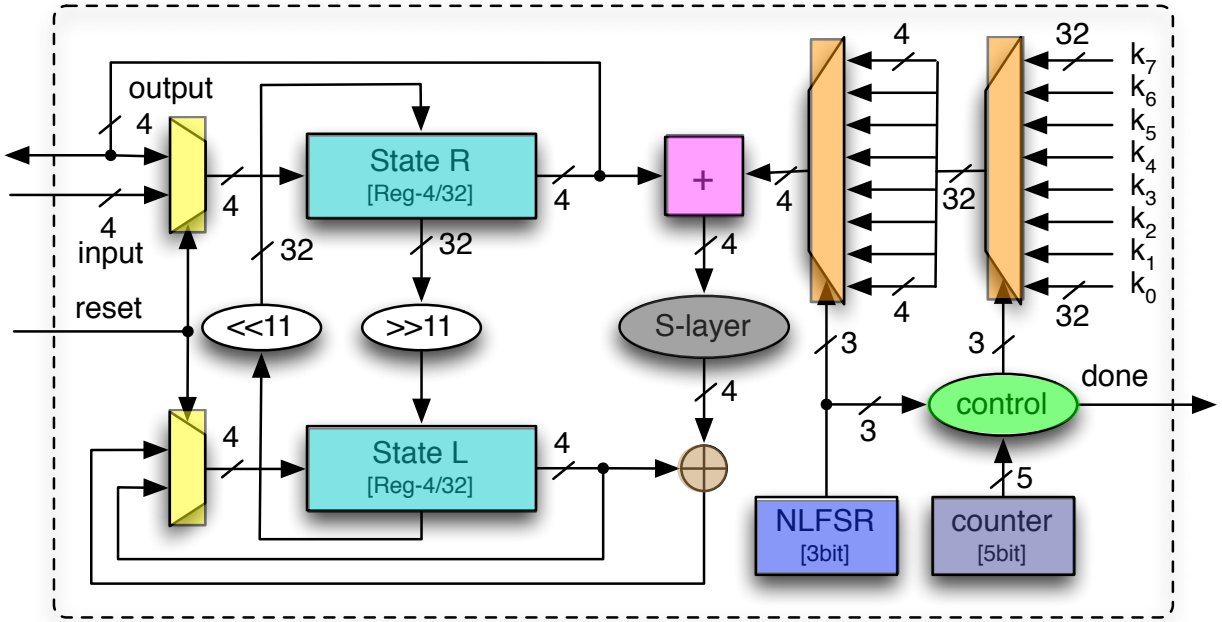
GOST-FB





GOST-PS

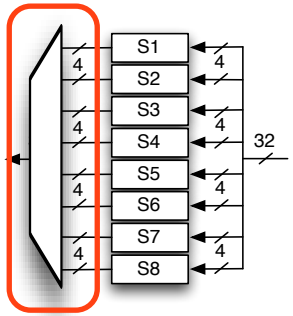




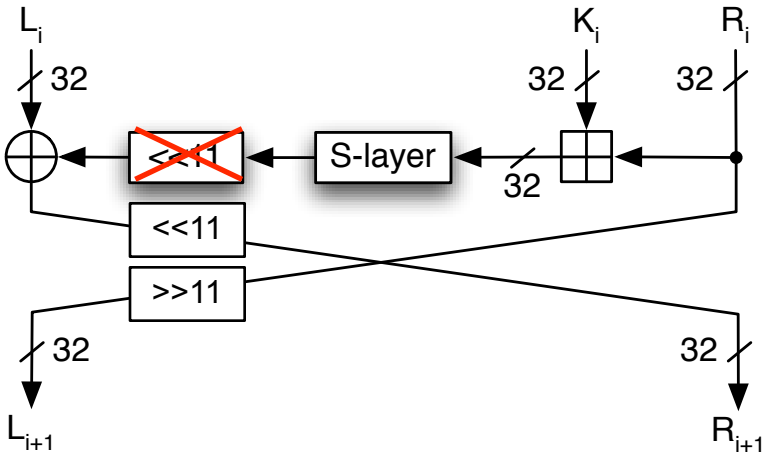
Implementation Results I

UMCL18G212T3 library

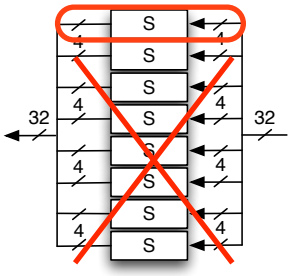
GOST-FB



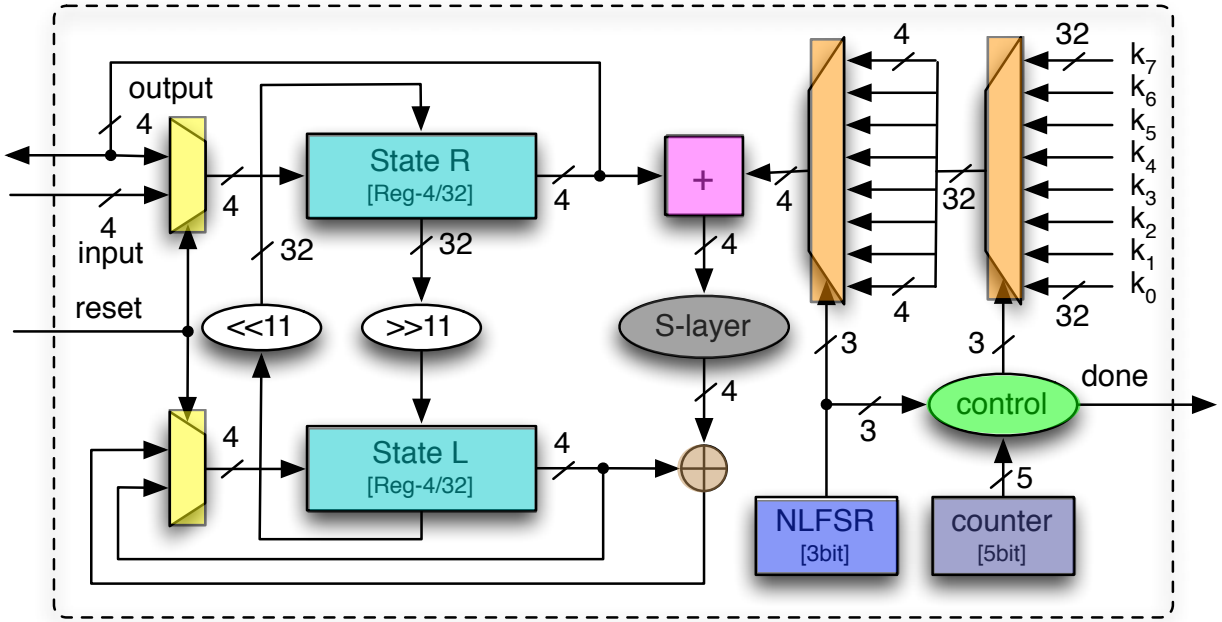
serial 264 CLK



GOST-PS



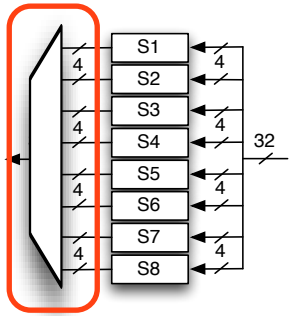
serial 264 CLK



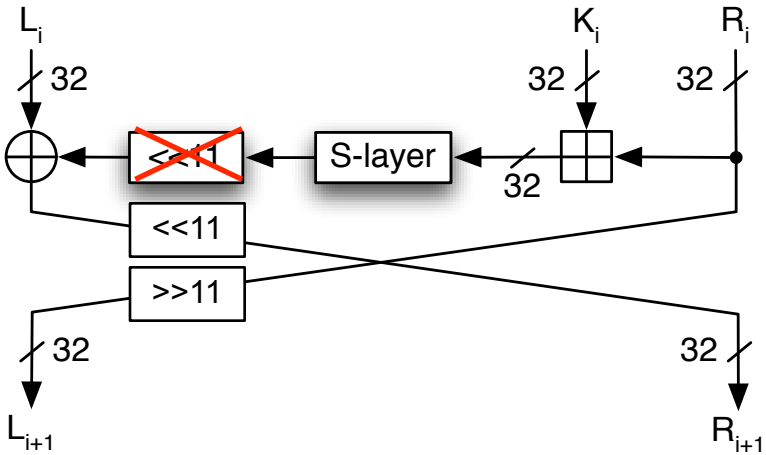
Implementation Results I

UMCL18G212T3 library

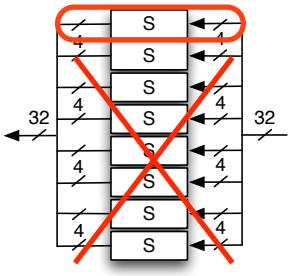
GOST-FB



serial 264 CLK

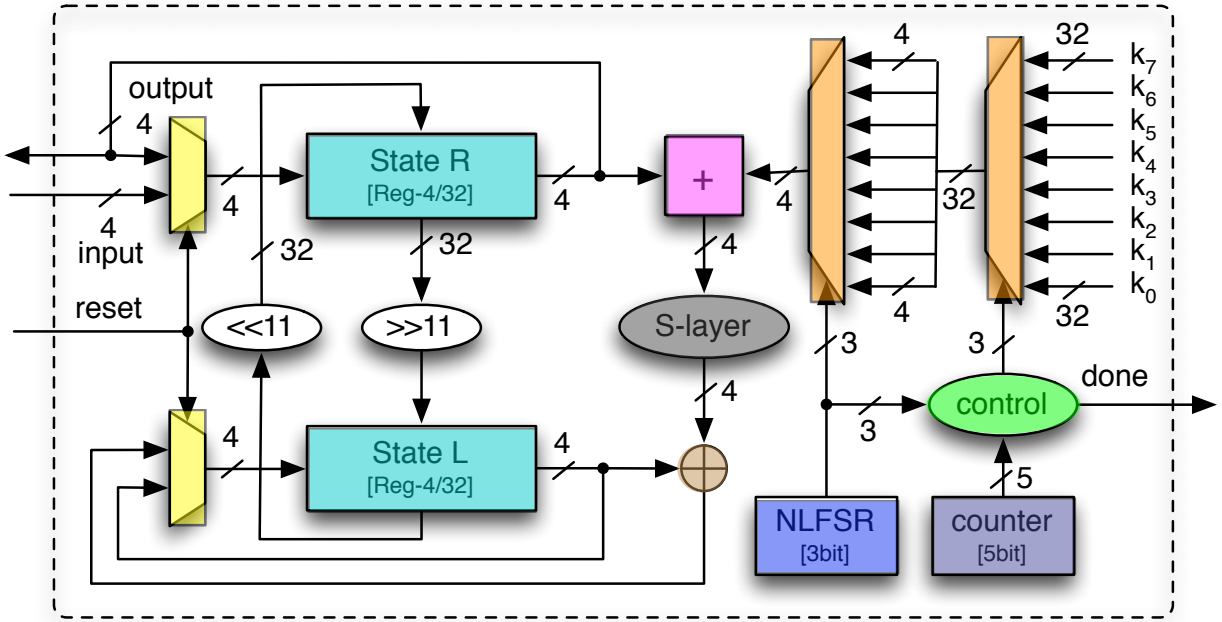


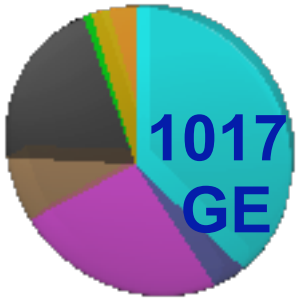
GOST-PS



serial 264 CLK

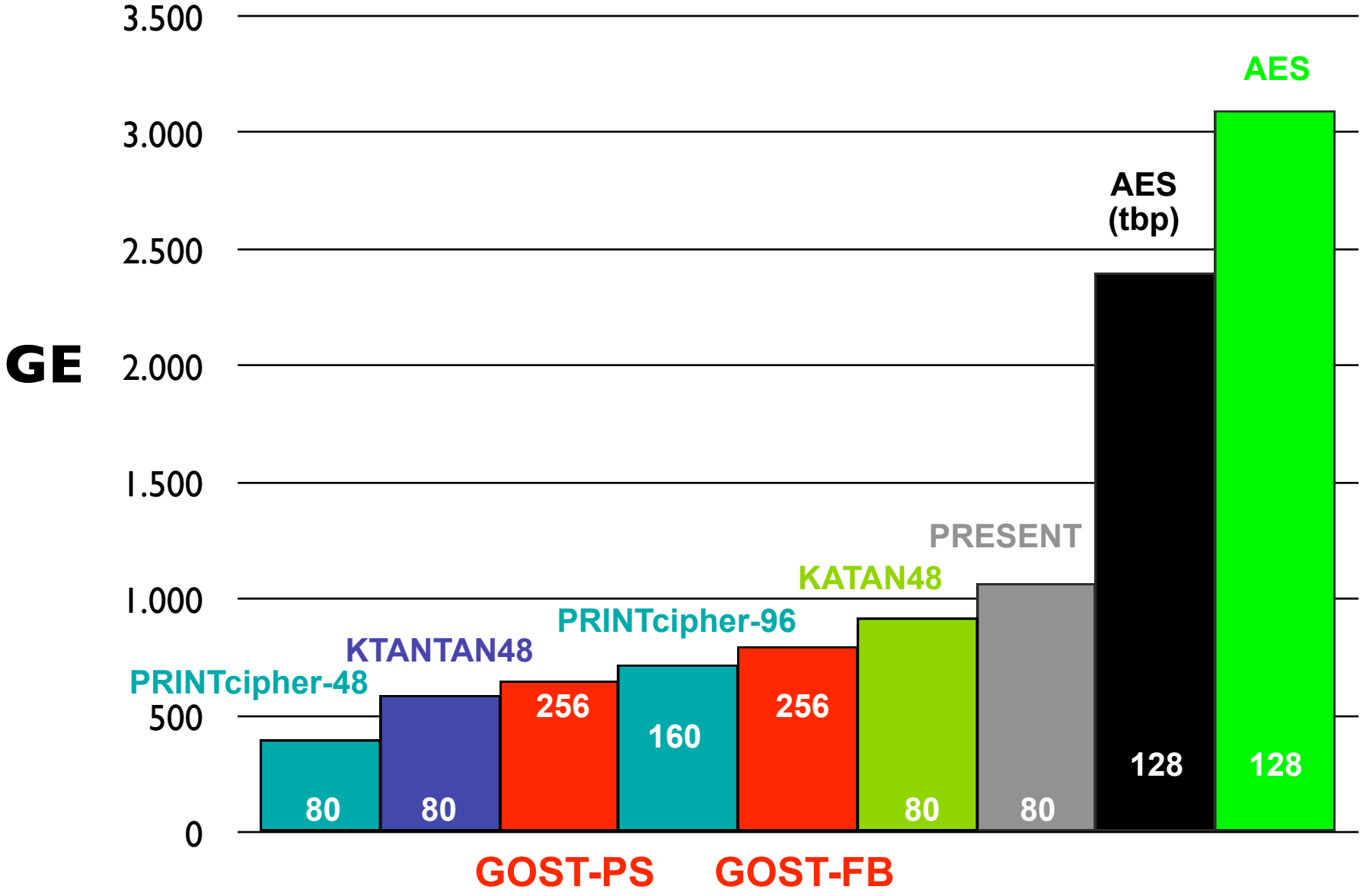
round 32 CLK





round 32 CLK

Implementation Results II



Outline

- Introduction
- GOST
- How to choose a set of S-boxes?
- Implementation Results
- **Conclusions**

Conclusions

- First hardware implementation of GOST 28147-89
- GOST 28147-89:
  - is standardized since 1989
  - survived 21 years of cryptanalysis
  - has a very compact hardware area footprint (651 GE)
  - has a key length of 256 bits

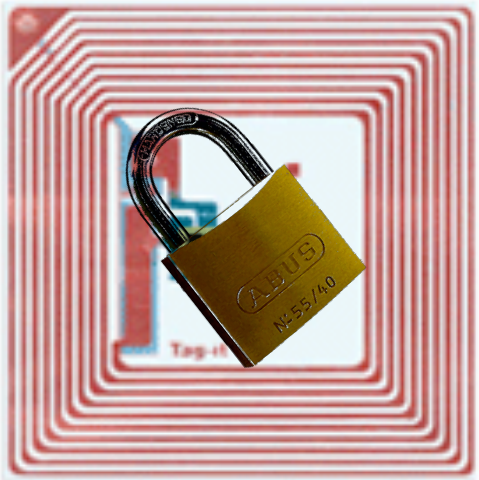
Conclusions

- First hardware implementation of GOST 28147-89
- GOST 28147-89:
  - is standardized since 1989
  - survived 21 years of cryptanalysis
  - has a very compact hardware area footprint (651 GE)
  - has a key length of 256 bits

GOST seems to be suitable for low-cost yet high secure applications

Thank you!

Questions?



Axel Poschmann
Division of Mathematical Sciences
Nanyang Technological University
SPMS-MAS-04-20, 50 Nanyang Avenue
Singapore 639798
T (65) 6513-7459 GMT+8h
E axel.poschmann@gmail.com
W www.ntu.edu.sg/home/aposchmann/